МРНТИ 10.77.01; 10.79.21 https://doi.org/10.26577/JAPJ2025115311

Қ.Р. Усеинова[1*], А.А. Тоқтыбаев[2], А.М. Жапарбек[1], С.Д. Данияров[1]

[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[2]Алматинская академия МВД Республики Казахстан имени М. Есболатова, Алматы, Казахстан
*e-mail: karlygash_usein@mail.ru

ДРОППЕРЫ КАК ИНСТРУМЕНТ КИБЕРПРЕСТУПНОСТИ: ИСТОРИЯ, ФУНКЦИИ, ВЫЗОВЫ ДЛЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Современное развитие цифровых технологий привело к появлению новых форм киберугроз, среди которых особое место занимает феномен «дропперов». В научной и практической литературе этот термин используется в двух значениях: во-первых, как программный компонент, обеспечивающий доставку и активацию иных вредоносных модулей; во-вторых, как лица или группы лиц, через которых проходят преступные средства, документы либо иные объекты противоправной деятельности. Такое двойственное понимание делает исследование дропперов актуальным и необходимым для формирования целостной системы правового реагирования.

Цель настоящего исследования заключается в комплексном анализе дропперов как инструмента киберпреступности, выявлении их функций и исторической эволюции, а также определении вызовов, которые они создают для правоохранительных органов Республики Казахстан. Основные направления работы сосредоточены на сравнении программных и социальных форм дропперов, изучении их роли в сокрытии источников преступной деятельности и выявлении правовых проблем их квалификации.

Научная и практическая значимость исследования проявляется в том, что рассмотрение дропперов позволяет по-новому взглянуть на механизмы функционирования киберпреступных схем и выработать рекомендации по совершенствованию законодательства и оперативно-розыскной деятельности. Методологическую основу составили общенаучные методы анализа, синтеза, системного и сравнительно-правового подхода, а также историко-правовой метод для изучения генезиса явления.

Результаты исследования подтверждают, что дропперы играют ключевую роль в усложнении раскрытия киберпреступлений, обеспечивая разрыв между исполнителями и конечными выгодоприобретателями. В работе предложены меры по усилению технического контроля, совершенствованию правового регулирования и повышению уровня правовой осведомлённости населения.

Вклад проведённого исследования заключается в расширении теоретического понимания киберугроз и разработке предложений, которые могут быть практически применены в деятельности правоохранительных органов Республики Казахстан.

Ключевые слова: дропперы, киберпреступность, посредники, информационные технологии, правовое регулирование, цифровая безопасность.

K.R. Useinova[1*], A.A. Toktybaev[2], A.M. Zhaparbek[1], S.D. Daniyarov[1]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbolatov, Almaty, Kazakhstan
*e-mail: karlygash_usein@mail.ru

Droppers as a tool of cybercrime: history, functions, and challenges for law enforcement agencies

The rapid development of digital technologies has led to the emergence of new forms of cyber threats, among which the phenomenon of “droppers” occupies a special place. In academic and practical literature, this term is used in two senses: first, as a software component designed to deliver and activate other malicious modules; second, as individuals or groups of individuals through whom illicit funds, documents, or other objects of criminal activity are channeled. This dual understanding makes the study of droppers both relevant and necessary for building a comprehensive system of legal response.

The purpose of this study is to provide a comprehensive analysis of droppers as a tool of cybercrime, to identify their functions and historical evolution, and to determine the challenges they pose to the law

enforcement agencies of the Republic of Kazakhstan. The main focus of the research lies in comparing the software and social forms of droppers, examining their role in concealing the sources of criminal activity, and identifying the legal difficulties of their qualification.

The scientific and practical significance of the study lies in the fact that the consideration of droppers allows for a fresh perspective on the mechanisms of cybercriminal schemes and contributes to the development of recommendations for improving legislation and investigative practice. The methodological framework of the research is based on general scientific methods of analysis, synthesis, systemic and comparative-legal approaches, as well as the historical-legal method applied to study the genesis of the phenomenon.

The findings confirm that droppers play a key role in complicating the disclosure of cybercrimes by creating a gap between perpetrators and ultimate beneficiaries. The study proposes measures to strengthen technical oversight, improve legal regulation, and raise the level of public legal awareness.

The contribution of this research lies in expanding the theoretical understanding of cyber threats and in developing proposals that can be practically applied in the activities of the law enforcement bodies of the Republic of Kazakhstan.

Keywords: droppers, cybercrime, intermediaries, information technologies, legal regulation, digital security.

К.Р. Усеинова[1*], А.А. Токтыбаев[2], А.М. Жапарбек[1], С.Д. Данияров[1]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[2]Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы, Алматы, Қазақстан
*e-mail: karlygash_usein@mail.ru

Дропперлер киберқылмыстың құралы ретінде: тарихы, функциялары, құқық қорғау органдары үшін ықпалдары

Цифрлық технологиялардың қарқынды дамуы жаңа киберқатерлердің пайда болуына әкелді, олардың ішінде ерекше орын алатын құбылыс – «дропперлер». Ғылыми және тәжірибелік әдебиеттерде бұл термин екі мағынада қолданылады: біріншіден, өзге зиянды модульдерді жеткізіп, іске қосуға арналған бағдарламалық компонент ретінде; екіншіден, қылмыстық жолмен алынған қаражаттар, құжаттар немесе өзге де заңсыз объектілер өтетін жеке тұлғалар немесе топтар ретінде. Мұндай қосарлы түсінік дропперлерді зерттеуді өзекті етеді және құқықтық әрекет етудің тұтас жүйесін қалыптастыру үшін қажет.

Осы зерттеудің мақсаты – дропперлерді киберқылмыстың құралы ретінде кешенді талдау, олардың функциялары мен тарихи эволюциясын анықтау, сондай-ақ олар Қазақстан Республикасы құқық қорғау органдарына туғызатын сын-қатерлерін айқындау. Жұмыстың негізгі бағыты дропперлердің бағдарламалық және әлеуметтік түрлерін салыстыруға, олардың қылмыстық әрекеттердің қайнар көздерін жасырудағы рөліне және құқықтық саралау мәселелерін анықтауға бағытталды.

Зерттеудің ғылыми және тәжірибелік маңыздылығы дропперлерді қарастыру киберқылмыстық схемалардың жұмыс істеу тетіктеріне жаңа көзқараспен қарауға мүмкіндік беріп, заңнаманы және жедел-іздестіру қызметін жетілдіруге арналған ұсыныстар жасауға ықпал ететінінде. Зерттеудің әдіснамалық негізін жалпығылыми талдау, синтез, жүйелік және салыстырмалы-құқықтық әдістер, сондай-ақ құбылыстың генезисін зерделеуге арналған тарихи-құқықтық әдіс құрады.

Зерттеу нәтижелері дропперлердің киберқылмыстарды әшкерелеуді күрделендірудегі негізгі рөлін дәлелдейді, олар орындаушылар мен түпкілікті пайда алушылардың арасындағы байланысты үзіп тұрады. Жұмыста техникалық бақылауды күшейту, құқықтық реттеуді жетілдіру және халықтың құқықтық сауаттылығын арттыруға бағытталған шаралар ұсынылды.

Зерттеудің қосқан үлесі киберқатерлер туралы теориялық түсінікті кеңейтуге және Қазақстан Республикасы құқық қорғау органдарының қызметінде тәжірибелік тұрғыдан қолдануға болатын ұсыныстар әзірлеуге негізделген.

Түйін сөздер: дропперлер, киберқылмыс, делдалдар, ақпараттық технологиялар, құқықтық реттеу, цифрлық қауіпсіздік.

Введение

Современные вызовы в сфере киберпреступности обусловлены стремительным развитием цифровых технологий и постоянной трансформацией способов, которыми злоумышленники реализуют противоправные замыслы. В этих условиях особое внимание научного сообщества и правоохранительных органов привлекает феномен так называемых «дропперов». Сам термин употребляется в двух различных плоскостях: в сфере информационной безопасности он обозна-

чает класс программных средств, предназначенных для скрытой доставки вредоносного кода; в криминологическом же контексте под «дропперами» понимаются физические лица или целые группы посредников, участвующие в переводе или сокрытии денежных средств, товаров или иных объектов преступления. Несмотря на то, что оба значения термина имеют разную природу, их объединяет общий признак – это функция «передачи» и «маскировки» противоправных действий (Ханов Т.А. 2017:72).

Актуальность изучения данного явления определяется несколькими факторами. Во-первых, универсальность дропперов как инструмента, они применяются в схемах мошенничества, вымогательства, незаконного доступа и отмывания доходов. Во-вторых, затруднённость правоприменительной практики, доказательство умысла, установление роли и степени участия требует сложных процедур, как цифровой экспертизы, так и анализа финансовых потоков. В-третьих, трансграничный характер киберпреступлений создаёт дополнительные проблемы для национальных правовых систем, поскольку как программные, так и человеческие дропперы часто функционируют в нескольких юрисдикциях одновременно.

В обоих случаях дроппер выступает не в роли конечного элемента преступления, а как промежуточное звено, без которого невозможно полноценное функционирование преступной схемы.

Во-первых, изучение феномена дропперов важно с точки зрения формирования национальной стратегии кибербезопасности. На практике дропперы становятся тем связующим элементом, который обеспечивает устойчивость преступной сети и позволяет организаторам избегать прямой ответственности. Их деятельность не ограничивается только финансовыми операциями, но они еще и задействованы в цепочках отмывания денег, незаконного оборота цифровых активов, криптовалютных переводов и даже в логистике поставок запрещённых товаров через теневые интернет-площадки. Такой спектр применения подчёркивает необходимость рассматривать дропперов как системный вызов, требующий многоуровневого правового и организационного ответа.

Во-вторых, исследование дропперов важно и с социальной точки зрения. Чаще всего в качестве посредников выступают молодые люди, студенты или социально уязвимые группы населения, для которых предложение «лёгкого заработка» становится фактором вовлечения в преступную деятельность. Недостаточный уровень правовой грамотности и финансовой культуры делает таких лиц особенно подверженными риску стать участниками криминальных схем. Это создаёт не только юридическую, но и социальную проблему, так как формирует слой «невольных соучастников», вовлечённых в преступления без полного понимания последствий.

В-третьих, актуальность изучения дропперов усиливается глобализацией киберпространства. Транснациональные преступные группы активно используют посредников в разных странах, что усложняет процесс расследования и требует международного взаимодействия правоохранительных органов. Для Казахстана эта проблема также приобретает практическое значение: географическое положение страны, её интеграция в мировую финансовую систему и рост цифровых сервисов создают условия, в которых схемы с использованием дропперов становятся всё более распространёнными. Это диктует необходимость не только адаптации национального законодательства, но и активного участия в международных инициативах по борьбе с киберпреступностью.

Обзор литературы

Изучение феномена дропперов в зарубежной научной литературе имеет два ключевых направления. Это исследования в области информационной безопасности и компьютерных наук, а также работы криминологов и специалистов по борьбе с организованной преступностью.

Первоначально внимание зарубежных исследователей было сосредоточено на технической природе дропперов как разновидности вредоносных программ. В классических работах по компьютерной безопасности (Skoudis 2003:325) дропперы рассматривались как отдельный класс, предназначенный для доставки более сложных компонентов, то есть вирусов или других шпионских программ. Эти труды заложили основы систематизации вредоносного кода, выделив дропперы как самостоятельный элемент в архитектуре киберугроз.

Более поздние публикации исследовали вопросы эволюции дропперов и их адаптации к современным условиям. Так, в работе Alazab (Alazab 2015:85-102) показано, что дропперы играют ключевую роль в скрытности атак и за-

трудняют обнаружение основной угрозы. В исследованиях последние годы внимание уделяется мультифункциональности дропперов, их способности использовать легитимные сервисы и методы стеганографии (Choo 2011: 719-731).

Наряду с технической стороной в зарубежной литературе заметно усилилось внимание к криминологическому измерению феномена. В ряде исследований (RUSI 2025:12) анализируется практика использования так называемых «money mules» или «drops» посредников, через которых проходят финансовые потоки преступного происхождения. Эти работы выявляют социальные и экономические факторы, способствующие вовлечению людей в подобные схемы, а также подчеркивают сложность международного расследования подобных преступлений.

Несмотря на значительные достижения, зарубежные исследования чаще всего рассматривают дропперов в рамках узких дисциплинарных подходов, либо исключительно как программные средства, либо как криминальную практику отмывания средств. При этом сравнительный анализ двух форм дропперов и их сопряжённого влияния на правовую систему отдельных государств, включая Республику Казахстан, в научной литературе до сих пор отсутствует. Именно восполнение этого пробела и составляет цель настоящего исследования, в котором предпринимается попытка связать технический и социально-правовой аспекты для выработки комплексного подхода к противодействию киберпреступности.

Методология

Вопрос исследования заключался в том, чтобы определить роль дропперов-посредников в современных формах киберпреступности и выявить проблемы, с которыми сталкиваются правоохранительные органы Республики Казахстан при расследовании подобных дел.

В качестве гипотезы было выдвинуто положение о том, что дропперы-посредники выступают ключевым звеном в преступных схемах, обеспечивающим анонимность организаторов и устойчивость преступных сетей. Предполагалось, что именно через них осуществляется значительная часть финансовых операций, связанных с отмыванием доходов от киберпреступлений, а значит, без учёта этой специфики невозможно выработать эффективные меры противодействия (https://zakonata.kz/dropperi-kto-eto/).

Этапы исследования включали:

1. Анализ зарубежной и отечественной научной литературы, а также официальных отчётов международных организаций. В частности, были изучены ежегодные обзоры Europol IOCTA (2019–2024 гг.) (Europol 2024:95) и ENISA Threat Landscape Reports (ENISA 2024:122).

2. Систематизацию судебной и следственной практики, опубликованной в открытых источниках, где рассматривались случаи привлечения «money mules».

3. Сравнительный анализ нормативного регулирования и доктринальных подходов в зарубежных странах (ЕС, США, Великобритания) и в Казахстане.

4. Обобщение полученных данных и выработка предложений по совершенствованию национальной правовой политики.

Методы исследования включали сравнительно-правовой анализ, историко-правовой подход, системный метод и криминологический анализ. Для количественного наполнения применялся контент-анализ статистических и аналитических источников.

Статистическая база исследования представлена:

- по данным Europol, только в 2023 г. в Европе выявлено свыше **10 000 случаев использования «money mules»**, связанных с отмыванием доходов от киберпреступлений (Europol 2024);

- по сведениям ENISA, более **70 % крупных киберпреступных схем** включают посредников для перевода средств и сокрытия цифровых следов (ENISA 2024);

- в Казахстане, согласно данным Комитета по правовой статистике Генеральной прокуратуры РК, в период 2021–2023 гг. зарегистрировано свыше **450 уголовных дел**, связанных с кибермошенничеством, при этом значительная их часть сопровождалась использованием посредников в переводе средств (Генеральная прокуратура Республики Казахстан. Статистика зарегистрированных уголовных дел по фактам кибермошенничества 2024).

Новизна методологии состоит в комплексном соединении юридического анализа и криминологических подходов с использованием как количественных, так и качественных данных. Это позволило подтвердить достоверность выводов и предложить практические меры, адаптированные к национальным условиям Казахстана.

Основная часть

Исторически понятие дроппера как программного компонента сформировалось в конце XX – начале XXI века, когда резкое усиление мер защиты вынудило разработчиков вредоносного программного обеспечения искать новые пути проникновения в информационные системы. В юридическом и социальном измерении феномен дропперов как посредников связан с развитием дистанционных финансовых сервисов и расширением теневых схем обналичивания средств, что породило устойчивую криминальную практику использования подставных лиц и реквизитов. То есть дропперы – это лица, предоставляющие мошенникам собственные банковские карты, счета или электронные кошельки для вывода денежных средств, полученных преступным путём. Они облегчают преступникам процесс легализации похищенных денег, выступая в роли посредников, которыми пользуются для снятия или перевода средств для дальнейшего распределения. Важно отметить, что дропперы могут не осознавать полную суть своей роли и участвовать в преступлениях без злого умысла, однако юридически они несут ответственность как соучастники (https://www.zakon.kz/).

История дропперов как явления киберпреступности связана с эволюцией цифровых технологий и развитием интернет-мошенничества. Появление дропперов напрямую связано с необходимостью преступников скрывать своё участие в финансовых преступлениях, связанных с хищением денежных средств через электронные каналы. Первые случаи использования дропперов отмечаются в начале 2000-х годов, когда массовое распространение онлайн-банкинга и электронных платёжных систем создало новые возможности для совершения киберпреступлений.

В то время мошенники столкнулись с ростом систем безопасности банков и усложнением прямых атак на счета жертв. Для обхода этих мер была придумана схема, при которой для снятия и перевода украденных денег стали использоваться «подставные» лица – дропперы. Они выступали в роли посредников, предоставляя свои реквизиты и действуя в интересах преступников, но, формально не являясь организаторами преступлений. Эта схема позволяла мошенникам сохранять анонимность и снижать риск быть идентифицированными.

С развитием интернета и финансовых технологий в 2010-х годах дропперы приобрели особую актуальность в странах с быстрорастущим цифровым рынком. В Казахстане активизация дропперства совпала с ростом популярности электронных кошельков и онлайн-услуг с начала 2010-х годов. Стремительное цифровое развитие финансовой системы Казахстана создало много возможностей для злоумышленников, которые начали активно вовлекать в схемы дропперов, часто среди молодежи и социально уязвимых групп.

В последние годы дропперство в Казахстане приобрело тревожные масштабы, сопровождаясь резким увеличением случаев кибермошенничества и финансовых преступлений с применением сложных цифровых схем. Правоохранительные органы уделяют особое внимание выявлению и пресечению деятельности дропперов, так как именно через них криминальные доходы выводятся в легальный оборот. Запросы на ужесточение законов и совершенствование механизмов борьбы с дропперами усилились к 2025 году, что отражает серьёзность и актуальность проблемы в условиях цифровой экономики Казахстана.

Функции дропперов заключаются в предоставлении своих реквизитов и действий с денежными средствами, переведёнными на них мошенниками. Они снимают деньги в банкоматах, делают переводы на другие счета или электронные кошельки, обеспечивая тем самым «отмывание» и перемещение незаконных средств. Это создаёт дистанцию между организаторами преступления и фактами его совершения, усложняя работу правоохранительных органов по выявлению и задержанию истинных преступников. При этом дропперы получают определённый процент от суммы за свои услуги. Часто дропперы выступают «наёмниками», которые не имеют доступа к полной информации о происхождении средств, но на них возлагается юридическая ответственность в соответствии с уголовным законодательством Республики Казахстан .

С 16 сентября 2025 года в Республике Казахстан прямо установлена уголовная ответственность за дропперство новой статьей 232-1 Уголовного кодекса Республики Казахстан. Норма введена Законом от 16 июля 2025 года № 210-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам оптимизации уголовного законодательства Республики Казахстан», который официально вступил в силу 16 сентября 2025 года (Закон Республики Казахстан от 16 июля 2025 г. № 210-VIII). Под дропперством

закон понимает, в частности, незаконное предоставление, передачу или приобретение доступа к банковскому счёту, платёжному инструменту либо идентификационному средству, а также осуществление незаконных платежей и/или переводов денег, в том числе в интересах третьих лиц за вознаграждение. За такие действия предусмотрены наказания от штрафа до лишения свободы до 7 лет, в ряде случаев – с конфискацией имущества.

Помимо прямого участия дропперов в обналичивании средств, важное значение имеет их роль в построении многоуровневых преступных сетей. Нередко дропперы формируют целые цепочки, где деньги проходят через несколько посредников, прежде чем достигают конечного получателя. Такая практика многократно усложняет процесс отслеживания транзакций и требует от правоохранительных органов использования более сложных инструментов финансового мониторинга. В мировой практике фиксируются случаи, когда через сеть дропперов средства переводились в десятки стран в течение нескольких суток, что практически исключало возможность оперативного реагирования. Для Казахстана эти схемы также становятся характерными, особенно в условиях активного развития международных переводов и платёжных сервисов.

Криминологический анализ показывает, что к дропперству чаще всего привлекаются лица, находящиеся в социально уязвимом положении. Это студенты, безработные, граждане с низким уровнем правовой грамотности. Преступные группы активно используют методы психологического давления или обещания лёгкой финансовой выгоды, что способствует вовлечению в противоправную деятельность всё новых участников. Нередко рекрутирование дропперов осуществляется через социальные сети, где публикуются объявления о «подработке» с быстрым доходом. Такая практика демонстрирует необходимость развития профилактических мер не только законодательных, но и информационно-просветительских, направленных на повышение уровня правовой культуры и цифровой безопасности населения (Васильева 2023:90).

Особую проблему представляет трансграничный характер деятельности дропперов. Если в начале 2010-х годов их действия ограничивались в основном внутренними переводами, то в последние годы значительная часть операций носит международный характер. Это означает, что расследование таких преступлений требует тесного взаимодействия Казахстана с зарубежными финансовыми организациями и правоохранительными структурами. Отсутствие единых подходов к определению и квалификации дропперства в разных правовых системах усложняет процесс экстрадиции и правовой помощи. В этих условиях перспективным направлением является гармонизация законодательства и участие Казахстана в международных инициативах по борьбе с киберпреступностью, что позволит выстраивать эффективные механизмы пресечения деятельности дропперов за пределами страны.

Результаты и обсуждение

Юридическая природа новых составов такова, что дроппер в этих схемах является самостоятельным субъектом преступления. Его действия квалифицируются не как «пассивная услуга», а как активное содействие трансформации и движения преступных доходов. С введением статьи 232-1 отпадает прежняя проблема, когда дропперы часто проходили по делам как свидетели либо приходилось «притягивать» к общим нормам о мошенничестве или легализации, что требовало доказывать прямой умысел на хищение или отмывание (Уголовный Кодекс РК). Теперь сам факт незаконной передачи/приобретения доступа, а также исполнения переводов за вознаграждение образует отдельный состав, и ответственности недостаточно избежать ссылкой на «неосведомлённость».

Важно понимать и границы применения новой нормы. Во-первых, действует общий принцип отсутствия обратной силы: ответственность по ст. 232-1 наступает за деяния, совершённые после 16 сентября 2025 г. Во-вторых, при наличии «надстройки» в виде хищения или организованной схемы возможна реальная совокупность со смежными составами (мошенничество; организация, руководство и участие в организованной преступной группе; легализация преступных доходов) – выбор квалификации будет зависеть от роли лица, объёма умысла и доказанной цепочки операций. Разъяснительные материалы Министерства внутренних дел РК подчёркивают дифференциацию санкций, то есть наиболее строгие пределы наказания применимы к организаторам «доступов», мягче – к тем, кто «сдаёт» доступ к своему счёту или выполняет переводы по указанию третьих лиц.

С криминалистической стороны дропперы остаются уязвимым звеном схем. Именно их

операции, а именно обналичивание, каскадные переводы, покупка криптоактивов оставляют трассу, которую можно быстро фиксировать и связывать с мошенничеством (фишинговые обзвоны, «социнженерия», компрометация аккаунтов) (Кувшинова 2022:45-54). Министерство внутренних дел и Генеральная прокуратура уже приводят статистику. Так в 2025 году только по зафиксированным эпизодам выявлены сотни дропперов и десятки киберпреступных групп, а сумма заблокированных подозрительных транзакций исчисляется миллиардами тенге и эти данные используются как аргумент к ужесточению ответственности и активизации межведомственного обмена информацией.

Вызовы для правоохранительных органов в Казахстане в борьбе с дропперами весьма значительны. Во-первых, дропперы часто меняют свои данные и реквизиты, что затрудняет отслеживание денежных потоков и выделение преступной цепочки из множества транзакций. Во-вторых, социальная природа дропперов в рядах «подставных лиц» нередко оказываются молодые люди или лица, вовлечённые в преступную схему обманом. Это требует не только карательных мер, но и профилактических, включая просвещение населения о рисках и последствиях участия в подобных схемах. В-третьих, ограниченность международного сотрудничества по вопросам киберпреступности и необходимости обмена информацией по трансграничным финансовым операциям усложняет работу местных правоохранительных подразделений (Комитет национальной безопасности Республики Казахстан 2023).

Кроме того, для правоохранителей критически важна техническая оснащённость – использование современных цифровых технологий мониторинга, анализа больших данных и искусственного интеллекта позволяет выявлять транзакции и подозрительные действия дропперов. Однако такие системы требуют постоянного обновления и обучения сотрудников, что является дополнительным вызовом в условиях постоянно развивающихся преступных схем. Повышение квалификации, а также создание специализированных подразделений киберполиции в Казахстане стали ответом на эти вызовы.

Заключение

Результаты показали, что дропперы-посредники играют ключевую роль в преступных схемах. Именно они обеспечивают разрыв между организаторами и конечными выгодоприобретателями, из-за чего расследование становится более сложным. Зачастую такие лица вовлекаются в противоправную деятельность под давлением или из-за недостатка правовых знаний, что делает их уязвимым звеном в цепочке киберпреступлений.

Основной вывод исследования заключается в том, что эффективная борьба с использованием дропперов требует не только ужесточения уголовной ответственности, но и развития профилактических мер. К ним можно отнести повышение финансовой грамотности населения, информационные кампании о рисках участия в подобных схемах и усиление контроля за подозрительными транзакциями.

Перспективы дальнейшей работы связаны с более глубоким изучением практики привлечения дропперов, анализом международного опыта и выработкой предложений для национальной стратегии кибербезопасности. Практическая значимость исследования заключается в возможности его использования при совершенствовании деятельности правоохранительных органов Казахстана и создании программ по предупреждению вовлечения граждан в противоправные схемы.

Таким образом, дропперы как инструмент киберпреступности – это неотъемлемая часть современных финансовых мошеннических схем, которые представляют серьёзную угрозу безопасности и стабильности финансовой системы Казахстана. Борьба с ними требует комплексного подхода, включающего развитие законодательства, совершенствование технических возможностей правоохранительных органов, а также активную профилактическую работу среди граждан, чтобы не допустить вовлечения новых участников в преступный оборот.

Научная статья подготовлена в рамках реализации грантового финансирования по научным и (или) научно-техническим программам на 2025-2027 годы (Комитет науки Министерства науки и высшего образования Республики Казахстан), направленная на реализацию проекта ИРН AP26101531: «Разработка эффективных механизмов пресечения деятельности дропперов в условиях цифровой экономики: устранение правовых пробелов и противодействие преступным сетям».

Литература

Ханов Т.А., Нуркеев А.Ж. Противодействие киберпреступности в Республике Казахстан и зарубежных странах: криминологический и виктимологический аспекты / – 2017. -URL: https://cyberleninka.ru/article/n/protivodeystvie-kiberprestupnosti-v-respublike-kazahstan-i-zarubezhnyh-stranah-kriminologicheskiy-i-viktimologicheskiy-aspekty/viewer

Skoudis E., Zeltser L. Malware: Fighting Malicious Code. – Upper Saddle River, NJ: Prentice Hall PTR, 2003. – 768 p.

Alazab M. Malware Detection and Mitigation Techniques: Lessons from Past, Present and Future // Cybercrime and Cybersecurity. – 2015. – Vol. 7(3). – P. 85–102.

Choo K.-K.R. The Cyber Threat Landscape: Challenges and Future Research Directions // Computers & Security. – 2011. – Vol. 30(8). – P. 719–731.

Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. – The Hague: Europol, 2024. – 95 p.

RUSI. Following the Fraud: The Role of Money Mules. – London: Royal United Services Institute, 2025. – 54 p.

Дропперы – кто это простыми словами // Zakonata.kz. – 22 июня 2025. – URL: https://zakonata.kz/dropperi-kto-eto/

ENISA. ENISA Threat Landscape 2024. – Athens: European Union Agency for Cybersecurity, 2024. – 122 p.

Генеральная прокуратура Республики Казахстан. Статистика зарегистрированных уголовных дел по фактам кибермошенничества за 2021–2023 гг. – Астана, 2024.

Кто такие дропперы и как не стать жертвой мошенничества // Zakon.kz. – 2024. – 21 октября. – URL: https://www.zakon.kz/obshestvo/6453416-kto-takie-droppery-i-kak-ne-stat-zhertvoy-moshennichestva.html

Закон Республики Казахстан от 16 июля 2025 г. № 210-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам оптимизации уголовного законодательства Республики Казахстан» // Официальная газета «Егемен Қазақстан». – 2025.

Уголовный Кодекс Республики Казахстан // Кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК. – URL: https://adilet.zan.kz/rus/docs/K1400000226

Кувшинова В.С. Финансовые посредники в структуре киберпреступности: криминологический анализ // Вестник Санкт-Петербургского университета МВД России. – 2022. – №2. – С. 45–54.

Васильева А.В. Дропперы в системе киберпреступности: уголовно-правовые проблемы квалификации и перспективы законодательного регулирования// Журнал российского права. – 2023. – №11. – С. 90.

Комитет национальной безопасности Республики Казахстан. Ежегодный отчёт о состоянии киберугроз и мерах по их предотвращению. – Астана, 2023. – 78 с.

References

Khanov T.A., Nurkeev A.Zh. (2017) Protivodeistvie kiberprestupnosti v Respublike Kazakhstan i zarubezhnykh stranakh: kriminologicheskii i viktimologicheskii aspekty [Countering Cybercrime in the Republic of Kazakhstan and Foreign Countries: Criminological and Victimological Aspects]. Cyberleninka, available at: https://cyberleninka.ru/article/n/protivodeystvie-kiberprestupnosti-v-respublike-kazahstan-i-zarubezhnyh-stranah-kriminologicheskiy-i-viktimologicheskiy-aspekty/viewer

Skoudis E., Zeltser L. (2003) Malware: Fighting Malicious Code. Upper Saddle River, NJ: Prentice Hall PTR, 768 p.

Alazab M. (2015) Malware Detection and Mitigation Techniques: Lessons from Past, Present and Future. Cybercrime and Cybersecurity, vol. 7, №3, pp. 85–102.

Choo K.-K.R. (2011) The Cyber Threat Landscape: Challenges and Future Research Directions. Computers & Security, vol. 30, №8, pp. 719–731.

Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. – The Hague: Europol, 2024. – 95 p.

RUSI (2025) Following the Fraud: The Role of Money Mules. London: Royal United Services Institute, 54 p.

Dropppy – kto eto prostymi slovami [Droppers – Who Are They in Simple Terms] (2025). Zakonata.kz, June 22, available at: https://zakonata.kz/dropperi-kto-eto/

ENISA. ENISA Threat Landscape 2024. – Athens: European Union Agency for Cybersecurity, 2024. – 122 p.

General’naya prokuratura Respubliki Kazakhstan (2024) Statistika zaregistrirovannykh ugolovnykh del po faktam kibermoshennichestva za 2021–2023 gg. [Statistics on Registered Criminal Cases of Cyber Fraud for 2021–2023]. Astana.

Kto takie dropppy i kak ne stat’ zhertvoi moshennichestva [Who Are Droppers and How Not to Become a Victim of Fraud] (2024). Zakon.kz, October 21, available at: https://www.zakon.kz/obshestvo/6453416-kto-takie-droppery-i-kak-ne-stat-zhertvoy-moshennichestva.html

Zakon Respubliki Kazakhstan (2025) Zakon Respubliki Kazakhstan ot 16 iyulya 2025 g. № 210-VIII «O vnesenii izmenenii i dopolnenii v nekotorye zakonodatel’nye akty Respubliki Kazakhstan po voprosam optimizatsii ugolovnogo zakonodatel’stva Respubliki Kazakhstan» [Law of the Republic of Kazakhstan of July 16, 2025 № 210-VIII “On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Optimization of Criminal Legislation”]. Ofitsial’naya gazeta Egemen Qazaqstan.

Respublika Kazakhstan (2014) Ugolovnyi kodeks Respubliki Kazakhstan ot 3 iyulya 2014 goda №226-V ZRK [Criminal Code of the Republic of Kazakhstan of July 3, 2014. № 226-V ZRK], available at: https://adilet.zan.kz/rus/docs/K1400000226

Kuvshinova V.S. (2022) Finansovye posredniki v strukture kiberprestupnosti: kriminologicheskii analiz [Financial Intermediaries in the Structure of Cybercrime: A Criminological Analysis]. Vestnik Sankt-Peterburgskogo universiteta MVD Rossii [Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia], №2, pp. 45–54.

Vasil'eva A.V. (2023) Dropppy v sisteme kiberprestupnosti: ugolovno-pravovye problemy kvalifikatsii i perspektivy zakonodatel'nogo regulirovaniya [Droppers in the System of Cybercrime: Criminal Law Problems of Qualification and Prospects for Legislative Regulation]. Zhurnal rossiiskogo prava [Journal of Russian Law], №11, pp. 80.

Komitet natsional'noi bezopasnosti Respubliki Kazakhstan (2023) Ezhegodnyi otchet o sostoyanii kiberugroz i merakh po ikh predotvrashcheniyu [Annual Report on the State of Cyber Threats and Measures for Their Prevention]. Astana, 78 p.

Сведения об авторах:

Усеинова Карлыгаш Рахимжановна (корреспондент-автор) – к. ю. н., ассоциированный профессор, заведующая кафедрой теории и истории государства и права, конституционного и административного права Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: karlygash_usein@mail.ru).

Токтыбаев Асет Абирбекович – к. ю. н., старший преподаватель Алматинской академии МВД РК имени М. Есболатова (Алматы, Казахстан, e-mail: tamerlan.arslan.83@bk.ru).

Жапарбек Арайлым Макулбековна – м. ю. н., преподаватель кафедры теории и истории государства и права, конституционного и административного права Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: zhaparbiek@mail.ru).

Данияров Санжар Дауренович – докторант Казахского национального университета имени аль-Фараби, старший преподаватель (Алматы, Казахстан).

Information about authors:

Useinova Karlygash Rahimzhanovna (correspondent author) – Candidate of Law, Associate Professor, Head of the Department of Theory and History of State and Law, Constitutional and Administrative Law of the Al-Farabi Kazakh National University (Kazakhstan, Almaty, e-mail: karlygash_usein@mail.ru).

Toktybaev Asset Abirbekovich – Candidate of Law, senior lecturer at the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbolatov (Kazakhstan, Almaty, e-mail: tamerlan.arslan.83@bk.ru).

Zhaparbek Arailym Makulbekovna – Master of Law, Lecturer at the Department of Theory and History of State and Law, Constitutional and Administrative Law, Al-Farabi Kazakh National University (Kazakhstan, Almaty, e-mail: zhaparbiek@mail.ru).

Daniyarov Sanzhar Daurenovich – Doctoral student of the Al-Farabi Kazakh National University (Almaty, Kazakhstan).

Авторлар туралы мәлімет:

Қарлыгаш Рахымжанқызы Усейінова (құрылымдық жұмыс жөніндегі автор) – заң ғылымдарының докторы, доцент, Әл-Фараби атындағы Қазақ ұлттық университетінің мемлекет және құқық теориясы мен тарихы, конституциялық және әкімшілік құқық кафедрасының меңгерушісі (Қазақстан, Алматы, e-mail: karlygash_usein@mail.ru).

Тоқтыбаев Әсет Әбірбекұлы – заң ғылымдарының докторы, М.Есболатов атындағы Қазақстан Республикасы Ішкі істер министрлігінің Алматы академиясының аға оқытушысы (Қазақстан, Алматы, e-mail: tamerlan.arslan.83@bk.ru).

Жапарбек Арайлым Мақұлбекқызы – Әл-Фараби атындағы Қазақ ұлттық университетінің мемлекет және құқық теориясы мен тарихы, конституциялық және әкімшілік құқық кафедрасының оқытушысы, кіші заңгер (Қазақстан, Алматы, e-mail: zhaparbiek@mail.ru).

Данияров Санжар Дәуренұлы – Әл-Фараби атындағы Қазақ ұлттық университетінің докторанты, аға оқытушысы (Қазақстан, Алматы).

Поступило: 20 августа 2025 г.
Принято: 10 сентября 2025 г.